(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平7－44672

(43)公開日　平成７年(1995)２月14日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｋ　19/073				
17/00		Ｅ		
			Ｇ０６Ｋ　19/ 00	Ｐ

審査請求　未請求　請求項の数８　ＦＤ　（全 13 頁）

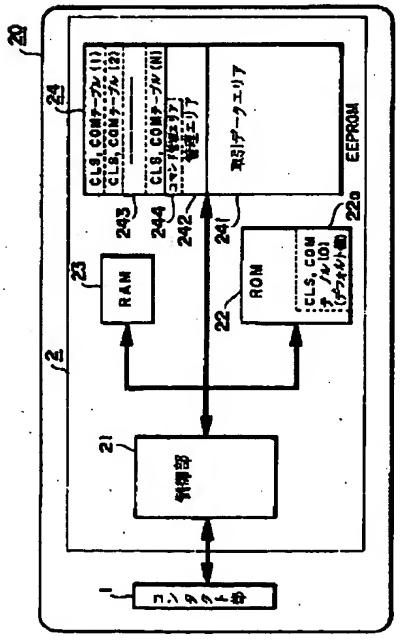
(21)出願番号　特願平5－205691

(22)出願日　平成５年(1993)７月28日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号
(72)発明者　正名　芳弘
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内
(74)代理人　弁理士　佐藤　幸男

(54)【発明の名称】　ＩＣカード及びＩＣカードシステム

(57)【要約】
【目的】　コマンドコードの機密性を高め、安全性を向上させる。
【構成】　上位装置はコンタクト部１を介してＩＣチップ２の制御部２１にライトコマンド、リードコマンド等のコマンドコードを送る。ＲＯＭ２２にはこれに対応したコマンドコードが格納されており、制御部２１はこれによりリードコマンド、ライトコマンド等のコマンドの種別を判別し、取引データエリア２４１内の取引データの読出し、書換え等を行う。この状態ではコマンド管理エリア２４４のコマンドテーブルの指定はＲＯＭ２２になっている。コマンドコードが第三者に知られたり、知られるおそれがあるときは、コマンド管理エリア２４４の指定を変えることにより、ＥＥＰＲＯＭ２４内のコマンドテーブルエリア２４３のコマンドテーブルを用いるようにする。



第１の実施例のＩＣカードの第１の実施例

1

【特許請求の範囲】

【請求項１】　書換え可能な不揮発性メモリ内に設けられた１又は２以上のコマンドテーブルから成るコマンドテーブルエリアと、
読出し専用の不揮発性メモリ内に設けられた書換え不能なコマンドテーブルと、
当該書換え不能なコマンドテーブル又は前記コマンドエリア内の１又は２以上のコマンドテーブルのうち、いずれか１つを指定するコマンド管理エリアとを備えたことを特徴とするＩＣカード。

【請求項２】　前記コマンド管理エリアは、各コマンドテーブルのいずれかを特定するため上位装置から送られた所定の番号と、コマンドテーブルの数とを格納し、当該コマンドテーブルの数が“０”の時は、前記読出し専用の不揮発性メモリ内に設けられた書換え不能なコマンドテーブルを指定し、当該コマンドテーブルの数が“０”以外の時は、前記所定の番号により特定される前記書換え可能な不揮発性メモリ内に設けられたコマンドテーブルを指定することを特徴とする請求項１記載のＩＣカード。

【請求項３】　前記コマンド管理エリアは、乱数と、コマンドテーブルの数とを格納し、当該コマンドテーブルの数が“０”の時は、前記読出し専用の不揮発性メモリ内に設けられた書換え不能なコマンドテーブルを指定し、当該コマンドテーブルの数が“０”以外の時は、前記乱数により特定される前記書換え可能な不揮発性メモリ内に設けられたコマンドテーブルを指定し、当該乱数を上位装置に通知することを特徴とする請求項１記載のＩＣカード。

【請求項４】　前記コマンド管理エリアは、乱数と、コマンドテーブルの数とを格納し、当該コマンドテーブルの数が“０”の時は、前記読出し専用の不揮発性メモリ内に設けられた書換え不能なコマンドテーブルを指定し、当該コマンドテーブルの数が“０”以外の時に上位装置から各コマンドテーブルのいずれかを特定する所定の番号が送られてきた場合は、当該所定の番号を格納し、これにより特定される前記書換え可能な不揮発性メモリ内に設けられたコマンドテーブルを指定し、当該コマンドテーブルの数が“０”以外の時に上位装置から前記所定の番号が送られてこなかった場合は、前記乱数により特定される前記書換え可能な不揮発性メモリ内に設けられたコマンドテーブルを指定し、当該乱数を上位装置に通知することを特徴とする請求項１記載のＩＣカード。

【請求項５】　読出し専用の不揮発性メモリ内に設けられた書換え不能なコマンドテーブルと、
当該コマンドテーブルに格納される各コマンドが有効か無効かを判定するため、書換え可能な不揮発性メモリ内に設けられた複数のイネーブルフラグから成るコマンドイネーブルエリアと、

2

当該コマンドイネーブルエリアの各イネーブルフラグを上位装置の指示に従って変更するコマンド処理部と、
前記上位装置から送られたコマンドに対し、当該コマンドに対応するイネーブルフラグを参照し、当該イネーブルフラグが有効の時は、コマンド処理を実行し、当該イネーブルフラグが無効の時は、前記上位装置にエラーを通知するコマンド実行部とを備えたことを特徴とするＩＣカード。

【請求項６】　前記コマンドイネーブルエリアは、前記コマンドテーブルに格納された全てのコマンドを一括して有効又は無効にするオールイネーブルフラグを含み、
前記コマンド実行部は、前記上位装置からコマンドが送られた際、まず、当該オールイネーブルフラグを参照し、当該オールイネーブルフラグが有効の時は、前記イネーブルフラグが有効となっているコマンドの処理を実行し、当該オールイネーブルフラグが無効の時は、前記上位装置にエラーを通知することを特徴とする請求項５記載のＩＣカード。

【請求項７】　請求項１記載のＩＣカードと、
当該ＩＣカードのコマンド管理エリアが指定するコマンドテーブルを当該ＩＣカードを使用するごとに変更する上位装置とから成ることを特徴とするＩＣカードシステム。

【請求項８】　請求項６記載のＩＣカードと、
当該ＩＣカードに対するアクセスの開始時にコマンドイネーブルエリアのオールイネーブルフラグを有効にし、前記アクセスの終了時に前記オールイネーブルフラグを無効にする上位装置とから成ることを特徴とするＩＣカードシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、制御部、記憶部を含む集積回路を備え、データ読出しコマンド、データ書込みコマンド等のコマンドを上位装置より受けて、各種の処理を行うＩＣカード及びＩＣカードシステムに関するものである。

【０００２】

【従来の技術】従来、上位装置と接続して各種の処理を行うＩＣカードがある。このようなＩＣカードには、塩化ビニール等から成るカード基材の表面に上位装置との信号（データを含む）の授受を行うコンタクト部があり、内部にＩＣチップが埋設されている。図２は、従来のＩＣカードのブロック図を示す。図示のＩＣカード１０は、コンタクト部１とＩＣチップ２で構成されている。ＩＣチップ２は、マイクロプロセッサ等の制御部２１と、制御プログラム等を格納するＲＯＭ２２と、データ一時格納用のＲＡＭ２３と、ＥＥＰＲＯＭ２４等から構成される。ＥＥＰＲＯＭ２４は、ＩＣカードの取引きデータ等を記憶し、複数のエリアからなる取引データエリアと、その管理エリア等から成る。

3

【０００３】また、図３に、上記の構成の従来のＩＣカードの内部処理を示す。ＩＣカード１０に電源、クロックが供給され、リセット信号が入れられると、ステップＳ１に進み、各部が正常に動作するか否かのイニシャルチェックを行う。次に、通信パラメータや、プロトコルタイプ等のデータを通知（Ans. to Reset ）として出力し（ステップＳ２）、コマンド入力待ち（ステップＳ３）になる。ここで、上位装置より、コマンドクラス（ＣＬＳ）、コマンドコード（ＣＯＭ）、パラメータ及びデータから成るコマンド電文を受けると、ステップＳ４へ進む。そして、ＲＯＭ２２内に格納されているコマンドテーブル２２ａを参照し、各コマンド処理へ分岐し（ステップＳ５）、各種コマンド処理が実行される。ここではリード処理（ステップＳ６）、ライト処理（ステップＳ７）、キーチェック処理（ステップＳ８）のみ記載したが、実際には、その他の様々のコマンド処理があり、これらの処理はＣＬＳ、ＣＯＭの値により分岐され実行される。そして、その後、ステップＳ３の入力待ちに戻る。また、入力されたＣＬＳ、ＣＯＭがコマンドテーブル２２ａに存在しなかった場合には、ステップＳ５からステップＳ９に進みコマンドエラーレスポンスを出力して、ステップＳ３に戻る。

【０００４】以上説明したように、従来のＩＣカード１０は、上位装置よりコマンド電文を受けて、各種のコマンド処理を行うようになっている。そして、コマンドの分類に当たるコマンドクラス（ＣＬＳ）と各種処理の命令に相当するコマンドコード（ＣＯＭ）は、図２に示すＲＯＭ２２内にコマンドテーブル２２ａとして制御プログラムと共に格納され、固定の値になっている。

【０００５】

【発明が解決しようとする課題】しかしながら、上記構成のＩＣカードでは、コマンドクラス（ＣＬＳ）及びコマンドコード（ＣＯＭ）がＲＯＭ内にあるため固定であり、悪意を持った第三者が上位装置とＩＣカード間の通信をモニタしたり、ＩＣカードに直接アタックしたりすれば比較的容易にＣＬＳ及びＣＯＭが判明してしまう。そして、判明したＣＬＳ、ＣＯＭを使用して、ＩＣカード内のデータを改ざんすることによって、第三者にＩＣカードが悪用される可能性があった。また、ＣＬＳ、ＣＯＭが判明しないまでも、ＩＣカードへの間違ったアクセスにより、カードが使用不可になる可能性があった。従って、悪意を持った第三者に、ＣＬＳ及びＣＯＭがもれてしまった時は、ＲＯＭ内のＣＬＳ、ＣＯＭを変更しなければならない。その場合、ＣＬＳ及びＣＯＭが固定であるので、ＩＣチップのＲＯＭマスクを変更するためのコストがかかる上、今まで使用してきたＩＣカードが全て無駄になるという問題点があった。

【０００６】また、一方で、アプリケーションによっては、ＩＣカードのＲＯＭ内に用意されたコマンドの一部しか使用せず、使用しないコマンドを殺して使用不可能

4

にしておきたい場合も同様にＲＯＭマスクを変更しなければならなかった。更に、異なるＣＬＳ、ＣＯＭを使用しているＩＣカードのアプリケーションシステムを相乗りさせる等の場合も、１つのＣＬＳ、ＣＯＭに統一するか、システムソフトを両方のＣＬＳ、ＣＯＭに対応させるかで対処するしかなく、どちらもコストがかかる。従って、異なるＣＬＳ、ＣＯＭを使用するＩＣカードのアプリケーションシステムを後から相乗りさせることは困難であった。

【０００７】本発明は、上述した問題点を解決するためになされたもので、コマンドクラス及びコマンドモードの機密性を保つことができ、安全で、汎用性に富んだＩＣカード及びＩＣカードシステムを提供することを目的とする。

【０００８】

【課題を解決するための手段】第１の発明のＩＣカードは、書換え可能な不揮発性メモリ内に設けられた１又は２以上のコマンドテーブルから成るコマンドテーブルエリアと、読出し専用の不揮発性メモリ内に設けられた書換え不能なコマンドテーブルと、当該書換え不能なコマンドテーブル又は前記コマンドエリア内の１又は２以上のコマンドテーブルのうち、いずれか１つを指定するコマンド管理エリアとを備えたことを特徴とするものである。

【０００９】第２の発明のＩＣカードは、読出し専用の不揮発性メモリ内に設けられた書換え不能なコマンドテーブルと、当該コマンドテーブルに格納される各コマンドが有効か無効かを判定するため、書換え可能な不揮発性メモリ内に設けられた複数のイネーブルフラグから成るコマンドイネーブルエリアと、当該コマンドイネーブルエリアの各イネーブルフラグを上位装置の指示に従って変更するコマンド処理部と、前記上位装置から送られたコマンドに対し、当該コマンドに対応するイネーブルフラグを参照し、当該イネーブルフラグが有効の時は、コマンド処理を実行し、当該イネーブルフラグが無効の時は、前記上位装置にエラーを通知するコマンド実行部とを備えたことを特徴とするものである。

【００１０】

【作用】第１発明のＩＣカードにおいては、上位装置から送られたコマンドコードは最初は読出し専用の不揮発性メモリ内に設けられた書換え不能なコマンドテーブルにより判別される。この状態ではコマンド管理エリアの指定は、書換え不能なコマンドテーブルを指定するようになっている。一方、コマンドコードが第三者に知られたり、知られるおそれがあるときは、コマンド管理エリアの指定を変える。これにより、書換え可能な不揮発性メモリ内に設けられたコマンドテーブルによりコマンドコードを判別するようにする。これらのコマンドテーブルは、複数のうちから１つを選択するようにしてもよく、また、単数のコマンドテーブルの内容を書き換えて

5

使うようにしてもよい。第2発明のICカードにおいては、コマンドテーブルによるコマンドの判別時にコマンドイネーブルエリアのイネーブルフラグを参照することにより、当該イネーブルフラグが有効のコマンドのみを実行可能とする。

【0011】

【実施例】以下、本発明を図の実施例を用いて詳細に説明する。図1は、本発明の第1の発明のICカードの第1実施例を示すブロック図である。図1のICカード20においては、上位装置との信号（データを含む）の授受を行うコンタクト部1と、1又は2以上のICチップ2とがカード基材に内蔵されている。ICチップ2は、カード全体を制御するマイクロプロセッサ等から成る制御部21と、制御プログラム等を格納するROM22と、データを一時格納するためのRAM23と、取引きデータ等を格納するEEPROM24とで構成されている。ROM22内には、“0”番のコマンドテーブル（CLS、COMテーブル）22aが格納されている。一方、EEPROM24内には、複数のエリアから成る取引きデータを格納する取引きデータエリア241と、各エリアを管理する管理エリア242と、1又は2以上のコマンドテーブル（CLS、COMテーブル）から成るコマンドテーブルエリア243が存在する。コマンドテーブルエリア243は、“1”番～“N”番のテーブルに分かれている。

【0012】このようなICカード20に使用されるコマンドは、図4（a）の図表のように、コマンド番号により、その処理が決められている。即ち、“1”番～“N”番のテーブルそれぞれに、図4（b）に示すように、CLS1（243a）、COM1（243b）、CLS2（243c）、COM2（243d）、CLS3（243e）、COM3（243f）…と、コマンド番号“1”から順に、それぞれのCLSコードと、COMコードとが格納されている。そして、例えばテーブル番号“1”と“2”では、同じコマンド処理でも異なるCLS、COMコードとなっている。

【0013】ICカード20が各コマンド処理の判定をするには、コマンドテーブルの先頭から何番目に格納されているCLS、COMかで容易に判定できる。また、これらのコマンドテーブルは、特定のパスワードの許可等で追記又は変更できるようになっている。一方、管理エリア242内には、コマンドテーブルエリア243を管理するコマンド管理エリア244があり、コマンド管理エリア244には、図4（c）に示すように、内部のコマンドテーブルエリア243内に存在するテーブル数244aと現在指定されているテーブル番号（244b）が設けられている。

【0014】次に、上記構成のICカード20の動作について説明する。図5は、第1の発明の第1の実施例のICカードの処理手順を示すフローチャートである。本

6

発明のICカード20に電源、クロックが供給され、リセット信号が入れられると、ステップS10に進み、イニシャルチェックを行う。次にステップS11に進み、コマンド管理エリア244を調べ、ステップS12でテーブル数244aが“0”の時、つまりコマンドテーブルエリア243内にコマンドテーブルが存在しない時はステップS13に進み、TNの値を“0”にする（つまり、ROM内のコマンドテーブル22aを指定する。）。

【0015】一方、テーブル数244aが“0”でない時は、ステップS14へ進み、TNに現在指定されているテーブル番号（244b）の値を代入する。次に、ステップS13又はS14からステップS15へ進み、ICカードの通信仕様等を上位装置に伝える通知（Answer to Reset）を出力し、コマンド入力待ち（ステップS16）となる。この状態でコマンドが入力されると、ステップS17へ進み、TNの値の番号のコマンドテーブルを参照する。例えば、TN＝1なら“1”番のコマンドテーブルを参照する。これにより、各コマンド処理に分岐し（ステップS18）、リード処理（ステップS21）、ライト処理（ステップS22）、キーチェック処理（ステップS23）等の各種処理を行った後、ステップS16に戻る。ここで入力されたコマンドのCOM、CLSが、コマンドテーブルを変更するテーブル変更コマンドのCOM、CLSであった場合は、ステップS19に進み、コマンド管理エリア244内のテーブル番号（244b）を指定された番号に変更し、更に、TNの値をテーブル番号（244b）の値に変更し（ステップS20）、コマンド入力待ち（ステップS16）に戻り、次のコマンド入力を待つ。

【0016】次のコマンドからは、変更したテーブル番号に対応するCLS、COMで分岐する。また、ステップS18で入力されたCOM、CLSがTNの値の番号のコマンドテーブルに該当するものがなかった場合には、ステップS24に進み、コマンドエラーであることを上位装置に知らせるレスポンスを出力し、コマンド入力待ち（ステップS16）に戻る。このように、第1の発明の第1の実施例では、EEPROM24内に1又は2以上のCLS、COMテーブルを持つコマンドテーブルエリア243を設け、使用されるコマンドテーブルの番号を指定するテーブル変更コマンドを設けて、コマンドのCLS、COMの値を変更できるようにした。

【0017】次に、第1の発明の第2の実施例について説明する。第2の実施例では、コマンド管理エリア244内に、図4（d）に示すように、現在のコマンドテーブルエリア243内に存在するテーブル数244aとICカード20内で乱数を生成するために使用する乱数初期値244cを設けた。乱数初期値244cは、乱数（疑似乱数）を生成するのに使用し、乱数発生ごとに書き換えられる。図6は、前記第2の実施例のICカード

の動作を示すフローチャートである。電源、クロックが供給され、リセットがかけられると、第1の実施例と同様に、イニシャルチェック（ステップS30）、コマンド管理エリア244の参照（ステップS31）が行われる。次に、ステップS32で、コマンド管理エリア内のテーブル数244aが“0”の時（コマンドテーブルエリア243にコマンドテーブルが1つもない時）は、ステップS33に進み、実際に使用されるコマンドテーブル番号であるTNにROM22内のコマンドテーブル22aの番号である“0”を代入し、テーブル数244aが“0”でない時は、ステップS34へ進み、乱数初期値244cを使用して、“0”～“N”の整数の乱数RNを生成し、RNをTNに代入する（ステップS35）。この時、乱数初期値244cは次の乱数生成のために別の値に書き換えられる。

【0018】次に、ステップS33、S35からそれぞれ、ステップS36へ進み、ICカードの通信仕様を上位装置に知らせる通知（Ans. to Reset ）と使用するコマンドテーブルの番号であるTNを上位装置に出力し、コマンド入力待ち（S37）に入る。上位装置はこのTNにより、どのコマンドテーブルを使用するかを知ることができる。ここでコマンドが入力されるとステップS38へ進み、TNの値で指定されるコマンドテーブルを参照し、入力されたコマンドのCLS、COMの値と、指定されているコマンドテーブルのCLS、COMとを比較し、各種コマンド処理（ステップS40、S41、S42等）に分岐し（ステップS39）、コマンド入力待ち（ステップS37）に戻る。ただし、入力されたコマンドのCLS、COMに対し、指定されているコマンドテーブル内に該当するものがなかった場合、ステップS39からステップS43へ進み、コマンドエラーのレスポンスを出力してステップS37に戻る。以上のように、第1の発明の第2の実施例では、乱数を使用して毎回異なるコマンドテーブルを指定するようにしたので、第三者がCLS、COMを調べてICカードを悪用することを防止できる。

【0019】次に、第1の発明の第3の実施例について説明する。第3の実施例は、前記第1の実施例と第2の実施例を合わせたもので、コマンド管理エリア244は、第2の実施例と同様で図4（d）の構成になっている。また、図7は、第3の実施例のICカードの処理のフローチャートを示すもので、イニシャルチェックのステップS50からコマンド分岐のステップS59まで第2の実施例と同じであり、入力されたコマンドのCLS、COMにより、各種コマンド処理（S61、S62、S63）へ進み、コマンド入力待ち（S57）へ戻る。ただし、コマンドテーブルの番号を変更するテーブル変更コマンドが入力された場合には、ステップS60へ進み、TNに指定されたテーブル番号を代入し、コマンド入力待ちのステップS57に戻る。

【0020】この処理により、新しいコマンドテーブルに変更され、次のコマンドから新しく指定された番号のテーブルに従って、コマンド処理が分岐される。また、ステップS57で入力されたコマンドのCLS、COMが該当しなかった場合は、ステップS64へ進み、コマンドエラーのレスポンスを返す。

【0021】以上詳細に説明したように、本発明の第1の発明は、従来、ROM22内にあったコマンドテーブルをEEPROM24内にも設け、ROM22のマスク変更をすることなしに、コマンドテーブルを変更することを可能にし、更に、乱数やテーブル変更コマンドにより、定期的にコマンドテーブルを変更し、コマンドのCLS、COMが第三者に漏れるのを未然に防ぎ、セキュリティを向上するものである。これに対し、次に説明する第2の発明は、アプリケーション上で使用しないコマンドをROM22のマスク変更をすることなしに、選択的にコマンドを有効／無効にできるものである。

【0022】図8は、第2の発明のICカードの実施例を示すブロック図である。図8のICカード30は、コンタクト部1と、制御部21′、ROM22、RAM23、EEPROM24等から成る1又は2以上のICチップ2とで構成される。ROM22内には、制御プログラムと共に、コマンドテーブル22aが存在し、EEPROM24内には、複数のエリアから成る取引きデータを格納する取引データエリア241と各エリアを管理する管理エリア242と、各コマンドを有効／無効にするコマンドイネーブルエリア245が設けられている。コマンドイネーブルエリア245は、図9（a）に示すように、各コマンドを有効にするか無効にするかを決めるフラグ245aが設けられている。ここで、各コマンドには、図4（a）に示すようにコマンド番号が設けられており、この番号によりフラグ245aがどのコマンドに対応するかを判断する。つまり、例えば、“2”番のリードコマンドが入力された時は、先頭から2番目のフラグを見て、“1”ならば有効とし、リードコマンドを実行する。一方、そのフラグが“0”ならばリードコマンドを無効とし、リードコマンドが存在しないかのようにコマンドエラーのレスポンスを出力する。

【0023】制御部21′には、コマンド処理部211と、コマンド実行部212とが設けられている。コマンド処理部211は、所定のイネーブルフラグ変更コマンドの入力により、そのコマンドに指定されたフラグ245aを有効又は無効に変更する。コマンド実行部212は、イネーブルフラグ変更コマンド以外のコマンドの入力により、そのコマンドに対応したフラグ245aが有効の場合にそのコマンド処理を実行し、無効の場合にエラーレスポンスを出力する。

【0024】この第2の発明の第1の実施例のICカードの処理を示すのが図10のフローチャートである。ICカードに電源、クロックが供給され、リセット信号が

9

入れられると、イニシャルチェックを行い（ステップＳ７０）、通信仕様等を上位装置に伝える通知（Ans. to Reset ）を出力し（ステップＳ７１）、コマンド入力待ちのステップＳ７２に入る。ここで、コマンドが入力されると、まず、ＲＯＭ２２内のコマンドテーブル２２ａを参照し（ステップＳ７３）、該当するコマンドがあるかどうかを判断する（Ｓ７４）。該当するものがなかった場合は、ステップＳ７５へ進み、コマンドエラーレスポンスを出力し、コマンド入力待ち（ステップＳ７２）に戻る。もし、ステップＳ７４で該当するコマンドがあった場合には、ステップＳ７６へ進み、コマンドがコマンドイネーブルエリア２４５のフラグ２４５ａを変更するイネーブルフラグ変更コマンドであるか否かを判断する。イネーブルフラグ変更コマンドであった場合は、ステップＳ７７へ進み、指定されたイネーブルフラグを変更し、ステップＳ７２のコマンド入力待ちに戻る。

【００２５】一方、イネーブルフラグ変更コマンドでなかった場合は、コマンドイネーブルエリア２４５のイネーブルフラグ２４５ａを調べ（ステップＳ７８）、入力されたコマンドのイネーブルフラグが“１”なら入力されたコマンド処理（例えば、ステップＳ８０、Ｓ８１、Ｓ８２等）を行う。一方、入力されたコマンドのイネーブルフラグが“０”ならコマンドレスポンスエラーを出力し（ステップＳ８３）、コマンド入力待ちに戻る。

【００２６】以上のような動作により、イネーブルフラグ変更コマンドでイネーブルフラグを“０”にされたコマンドは、コマンドが用意されているにもかかわらず、外からは、そのコマンドが存在しないかのように見える。これにより、アプリケーションで使用しないコマンドを選択的に無効にできる。例えば、アプリケーションでは一般に使用しない発行用のコマンド等をカード発行後、無効にする等が容易にできる。また、第２の発明の第２の実施例では、コマンドイネーブルエリア２４５に更に、図９（ｂ）に示すように、コマンド全体を一括に有効／無効にするオールイネーブルフラグ２４５ｂを設けている。第２の発明の第２の実施例の処理手順を示すフローチャートは、図１０に示すフローチャートを以下のように変更したものとなる。図１０のステップＳ７９の部分で、前述したオールイネーブルフラグ２４５ｂが“０”の時は、全てのコマンドに対し、ステップＳ８３のコマンドエラーレスポンスを出力する。また、オールイネーブルフラグ２４５ｂが“１”の時は、イネーブルフラグ２４５ａに従って、各種コマンド処理を実行するかエラーレスポンスを出力するかを行う。この後、コマンド入力待ち（ステップＳ７２）に戻る。なお、オールイネーブルフラグ２４５ｂの変更のためのコマンドには、イネーブルフラグ変更コマンドで共用しても別途専用のコマンドを設けてもかまわない。

【００２７】第２の発明の第２の実施例のカードでは、アプリケーションシステムの上位装置が、カード使用の

10

最後でオールイネーブルフラグ２４５ｂを“０”にし、使用開始時に“１”に変更して使用すれば、悪意を持った第三者がＣＬＳ、ＣＯＭを調べるためにアタックしたり、データの改ざんを行おうとしても、オールイネーブルフラグ２４５ｂを変更するコマンドを知らなければ、ＩＣカードへのアタックが不可能となり、ＩＣカードの悪用を未然に防ぐことができる。

【００２８】以上、第１の発明及び第２の発明について詳細に説明してきたが、本発明は、上記の実施例に限定されるものではない。例えば、第１の発明では、現在の指定コマンドテーブル番号をＴＮという変数（ＲＡＭ２３上にある）にいったん格納して使用しているが、テーブル番号（２４４ｂ）をそのまま使用してもかまわない。また、第２、３の実施例でもテーブル番号（２４４ｂ）を設けて、乱数ＲＮをテーブル番号（２４４ｂ）に代入しても良い。

【００２９】また、第２の発明において、イネーブルフラグ２４５ａとオールイネーブルフラグ２４５ｂは“１”の時有効としたが、“０”の時有効とするものでもかまわない。また、イネーブルフラグ変更コマンドの判定（ステップＳ７６）をコマンドイネーブルエリア参照（ステップＳ７８）の前に行っているが、ステップＳ７９のコマンド分岐で同時に行っても良い。ただし、この場合は、イネーブル変更コマンドを無効にしてしまうと、２度と変更できなくなる可能性がある。特に、第２の実施例の場合、オールイネーブルフラグ２４５ｂを無効にしてしまうと、２度と使用できなくなるので、イネーブルフラグ変更コマンドの判定（ステップＳ７６）は、ステップＳ７８の前に行う必要がある。

【００３０】なお、第１の発明、第２の発明の両方において、実施例の各種コマンド処理の種類や処理内容等は、各実施例のものに限定されるわけではない。また、各実施例のコンタクト部１は、上位装置との信号の授受を行える手段であれば接触式に限定されるものではない。

【００３１】

【発明の効果】以上詳細に説明したように、第１の発明では、ＲＯＭ内のコマンドテーブル（ＣＬＳ、ＣＯＭテーブル）とは別に、ＥＥＰＲＯＭ内に１又は２以上のコマンドテーブルを持つコマンドテーブルエリアとコマンドテーブルを管理するコマンド管理エリアを設け、乱数又は上位装置からのコマンド処理で上記コマンドテーブルのうちの１つを指定できるようにしたので、ＩＣチップのＲＯＭマスクを変更せずにコマンドテーブルを変更でき、大幅なコスト低減が図れる上、定期的（第２、３の実施例では毎回）に、コマンドテーブルを変更できる。従って、ＣＬＳ、ＣＯＭが第三者に漏れることを防止でき、第三者によるデータ改ざん等の悪用を防止できる。また、第１及び第３の実施例では、上位装置からの指定でコマンドテーブルを変更できるため、異なるＣＬ

S、COMを使用しているＩＣカードのアプリケーションシステムにも容易に対応でき、後から相乗りさせることも可能である。

【００３２】一方、第２の発明の第１の実施例では、ＥＥＰＲＯＭ内にコマンドイネーブルエリアを設け、コマンドイネーブルエリア内に、各コマンドを有効／無効にするイネーブルフラグを設け、イネーブルフラグに従って各種コマンドを無効にできるようにしたので、アプリケーションで一部のコマンドのみ使用し、他を殺して使用不可能にしておきたい場合でも、ＲＯＭマスクを変更しないで対応できる。また、第２の実施例では、更に、コマンドイネーブルエリアに全コマンドを有効／無効にするオールイネーブルフラグを設けたので、アプリケーション使用終了時に、全コマンドを無効にしておけば、悪意を持った第三者がＣＬＳ、ＣＯＭを調べようとアタックしても、ＣＬＳ、ＣＯＭを解読できない上、カードへの間違ったアクセスによってカードが使用不可になるという問題を防止できる。

【図面の簡単な説明】

【図１】第１の発明のＩＣカードの各実施例のブロック図である。

【図２】従来のＩＣカードの一例のブロック図である。

【図３】従来のＩＣカードの内部処理手順のフローチャートである。

【図４】第１の発明に係るコマンドテーブル等の内容の説明図である。

【図５】第１の発明の第１の実施例の内部処理手順のフローチャートである。

【図６】第１の発明の第２の実施例の内部処理手順のフローチャートである。

【図７】第１の発明の第３の実施例の内部処理手順のフローチャートである。

【図８】第２の発明のＩＣカードの各実施例のブロック図である。

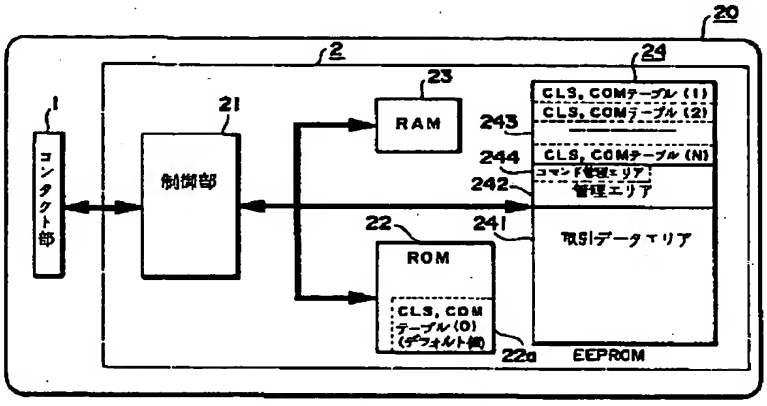
【図９】第２の発明に係るコマンドイネーブルエリアの内容の説明図である。

【図１０】第２の発明の第２の実施例の内部処理手順のフローチャートである。

【符号の説明】

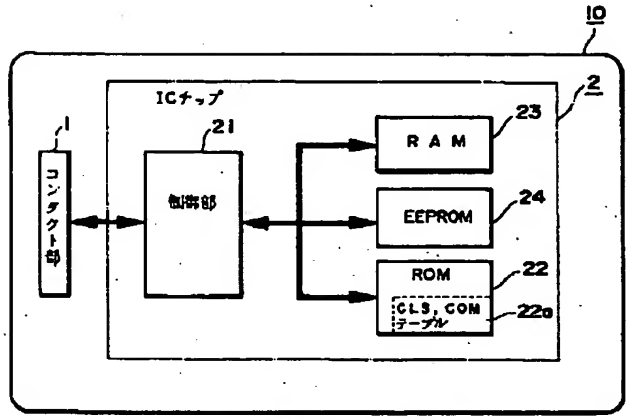
１　コンタクト部
２　ＩＣチップ
２１　制御部
２２　ＲＯＭ
２２ａ　コマンドテーブル
２３　ＲＡＭ
２４　ＥＥＰＲＯＭ
２４３　コマンドテーブルエリア
２４４　コマンド管理エリア

【図１】



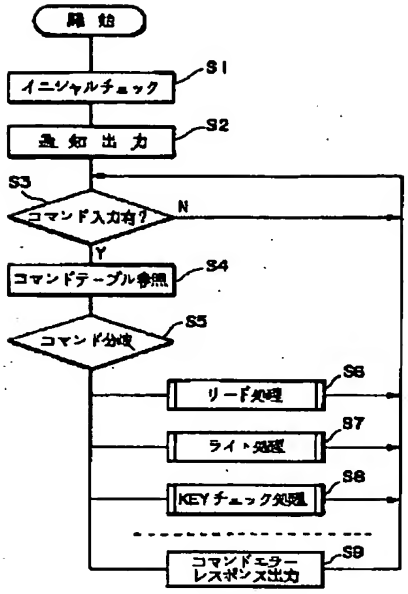
第１の発明のＩＣカードの第１の実施例

【図2】



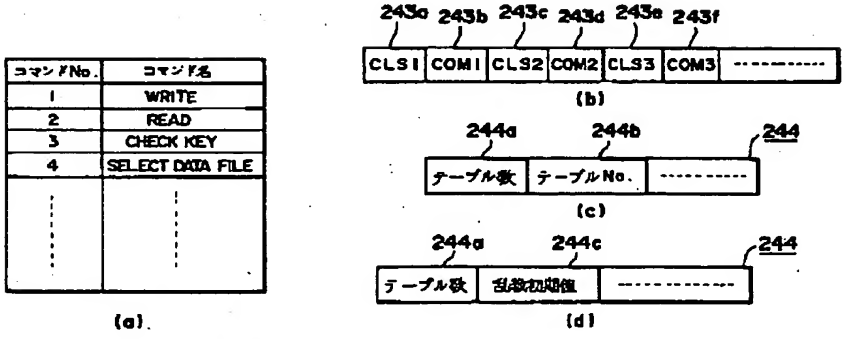
従来のICカードの一例

【図3】



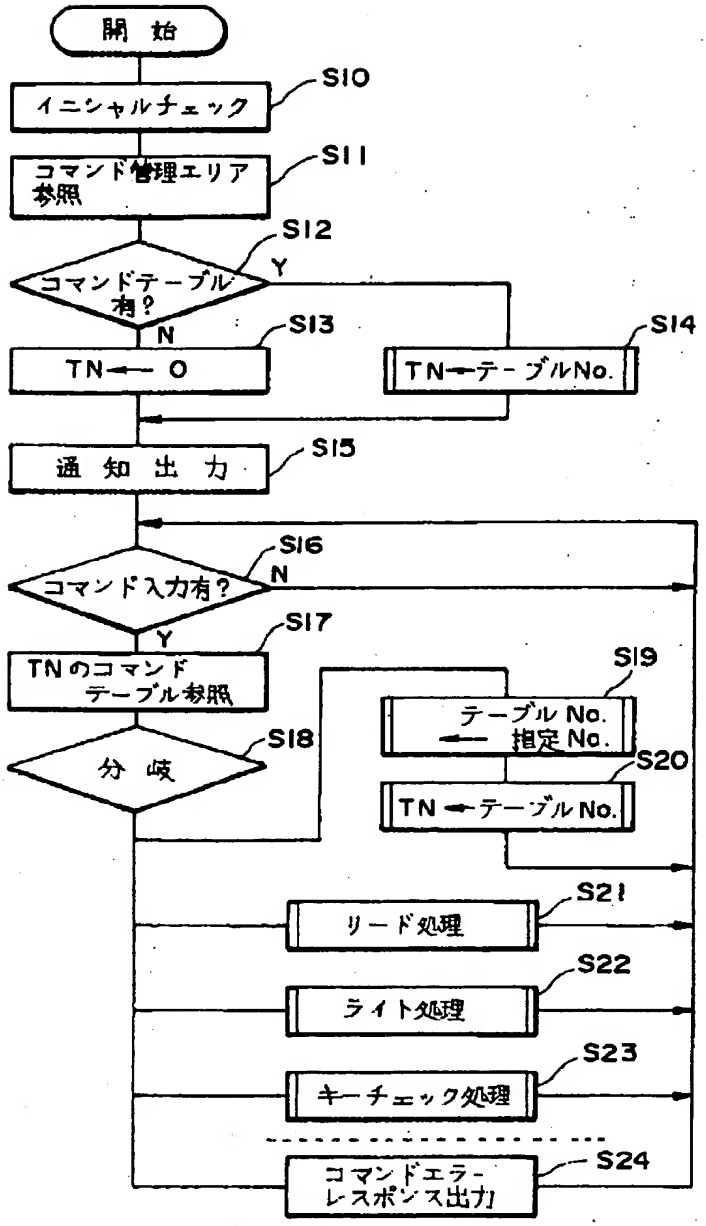
従来のICカードの内部処理手順

【図4】



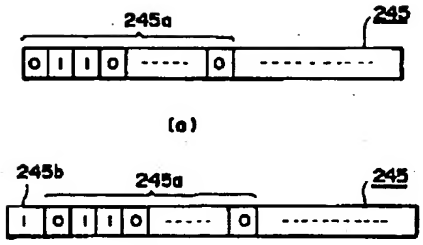
第1の発明に係るコマンドテーブル等の内容

【図5】



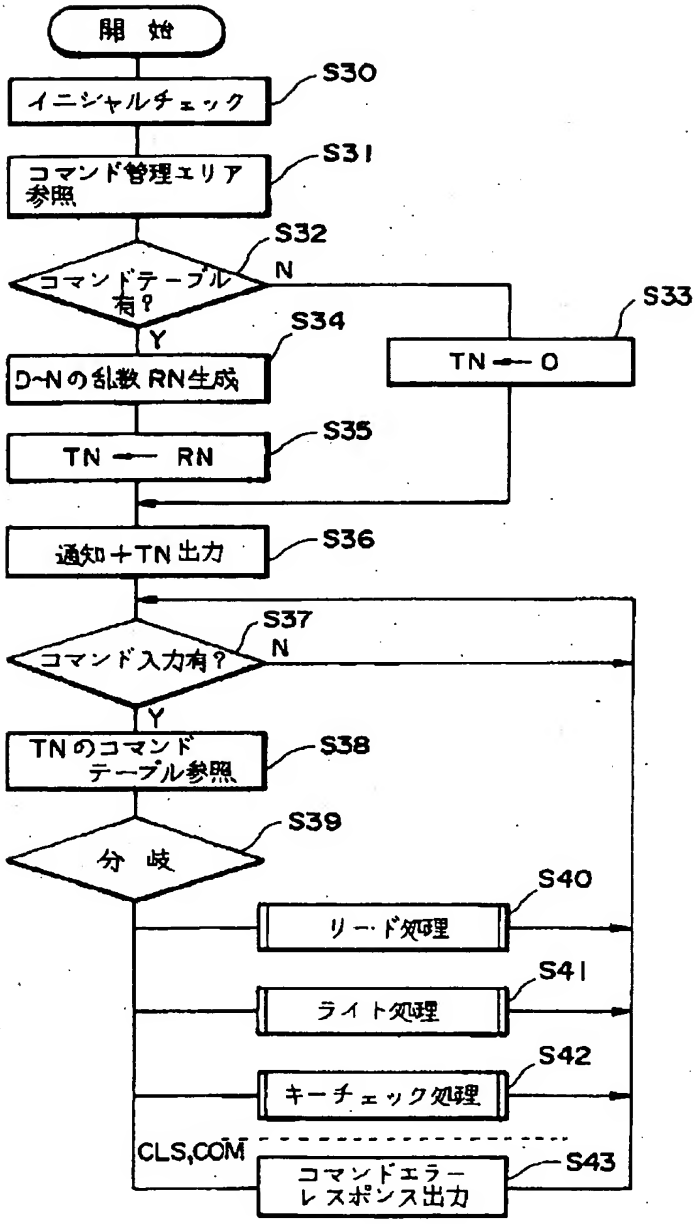
第1の発明の第1の実施例の内部処理手順

【図9】



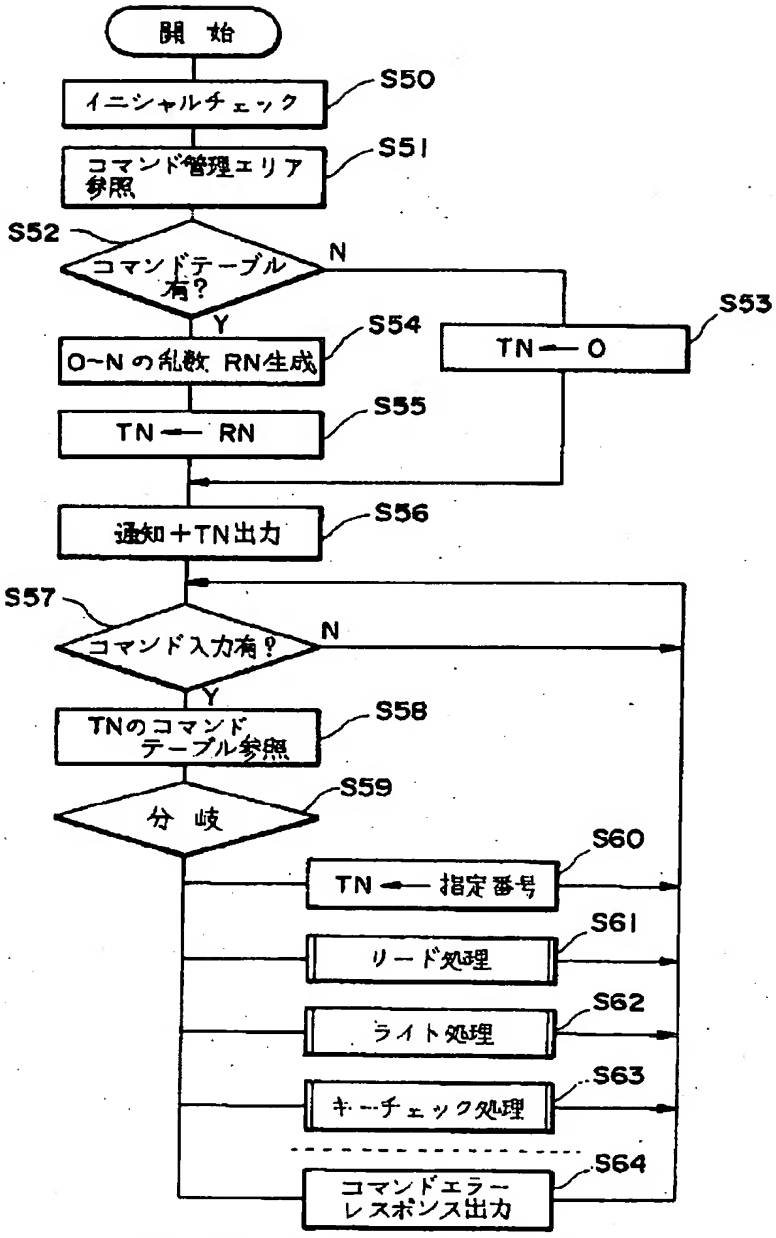
第2の発明に係るコマンドイネーブルエリアの内容

【図6】



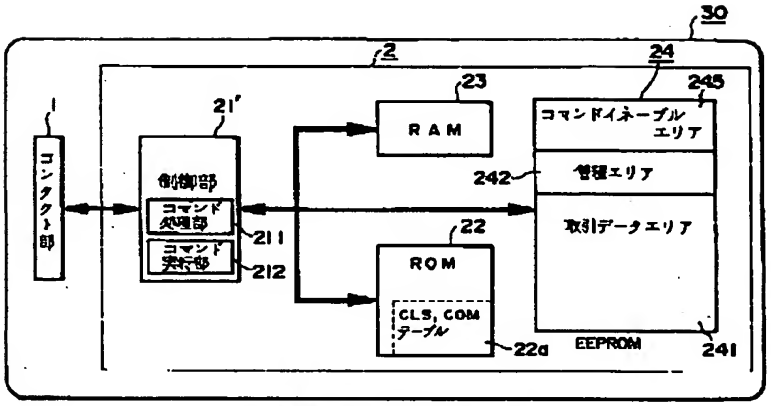
第1の発明の第2の実施例の内部処理手順

【図7】



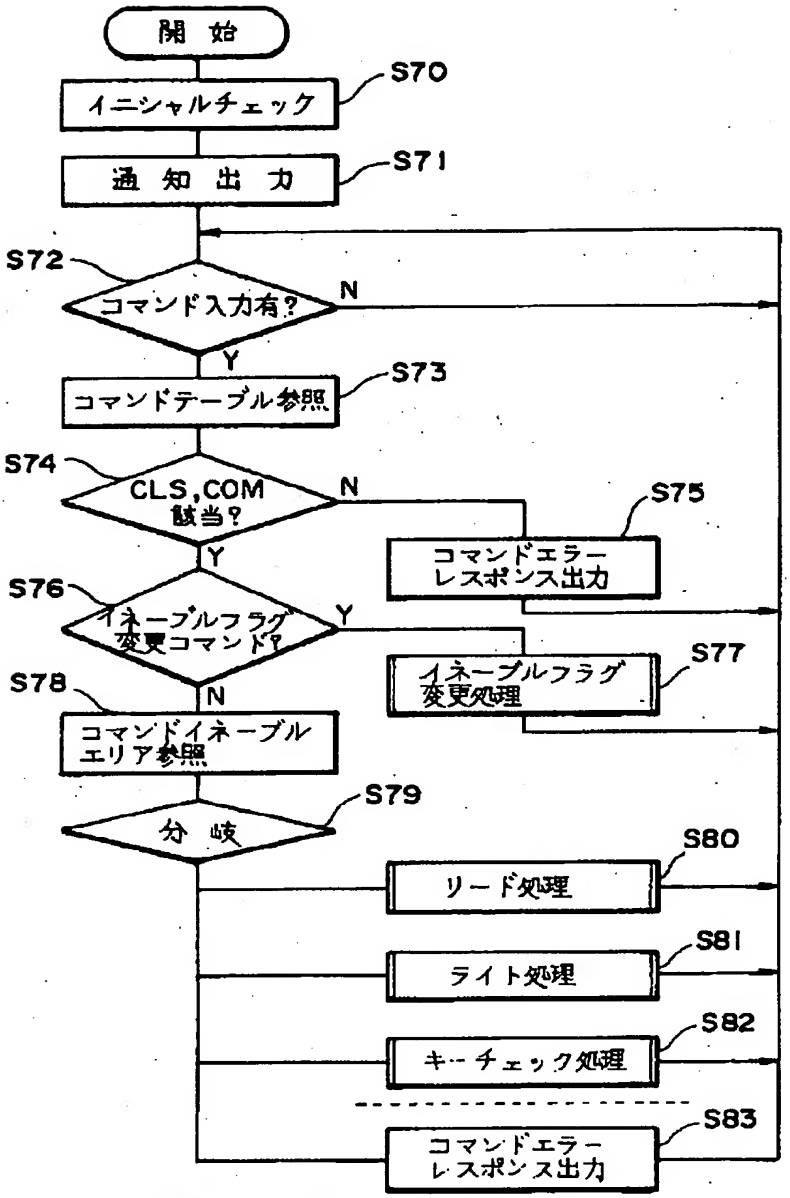
第1の発明の第3の実施例の内部処理手順

【図8】



第2の発明のICカードの各実施例

【図10】



第2の発明の第2の実施例の内部処理手順